Reports

Cisco ISE Reports

Cisco Identity Services Engine (ISE) reports are used with monitoring and troubleshooting features to analyze trends, and, monitor system performance and network activities from a central location.

Cisco ISE collects logs and configuration data from your network. It then aggregates the data into reports for you to view and analyze. Cisco ISE provides a standard set of predefined reports that you can use and customize to fit your needs.

Cisco ISE reports are pre-configured and grouped into categories with information related to authentication, session traffic, device administration, configuration, administration, and troubleshooting.

Related Topics

Run and View Reports, on page 3

Export Reports, on page 4

Available Reports, on page 7

Report Filters

There are two types of reports, single-section and multi-section. Single-section reports contain a single grid (Radius Authentications report) and multi-section reports contain many grids (Authentications Summary report) and represent data in the form of charts and tables. The Filter drop-down menu in the single-section reports contains the **Quick Filter** and **Advanced Filter**. In the multi-section reports, you can specify only advanced filters.

Multi-section reports may contain one or more mandatory advanced filters that require your input. For example, when you click the Health Summary report (**Operations > Reports > Diagnostics** page), it displays two mandatory advanced filters—Server and Time Range. You must specify the operator command, server name, required values for both these filters, and click **Go** to generate the report. You can add new advanced filters by clicking the Plus (+) symbol. You can export multi-section reports only in the PDF format. You cannot schedule Cisco ISE multi-section reports to run and re-run at specific time or time intervals.

Note When you click a report, data for the last seven days is generated by default. However, some multi-section reports require mandatory input from the user apart from the time range.

By default, the Quick Filter is displayed as the first row in single-section reports. The fields may contain a drop-down list from which you can select the search criteria or may be a text box.

An Advanced Filter contains an outer criteria that contains one or more inner criteria. The outer criteria is used to specify if the search should meet All or Any specified inner criteria. The inner criteria contains one or more conditions that is used to specify the Category (Endpoint ID, Identity Group) Method (operator commands, such as Contains, Does Not Contain), and Time Range for the condition.

When using the **Quick Filter**, you can choose a date or time from the **Logged At** drop-down list to generate reports for a data set logged in the last 30 days or less. If you want to generate a report for a date or time prior to 30 days, use the **Advanced Filter** to set the required time frame in the **From** and **To** fields of the **Custom** option from the drop-down list.

Create the Quick Filter Criteria

The section describes how to create a quick filter criteria. You can create quick filter criteria for only single-section reports.

Step 1 Choose **Operations** > **Reports** and click the required report.

Step 2 From the **Settings** drop-down list, choose the required fields.

Step 3 In the required field, you can choose from the drop-down list or type the specific characters to filter data. The search uses the Contains operator command. For example, to filter by text that begins with “K”, enter K or to filter text that has “geo” anywhere in the text, enter geo. You can also use asterisks (*), for example, the regex starting with *abc and ending with *def.

The quick filter uses the following conditions: contains, starts with, ends with, starts with or ends with, and multiple values with OR operator.

Step 4 Press **Enter**.

Create the Advanced Filter Criteria

The section describes how to create an advanced filter criteria. You can create advanced filters for single- and multi-section reports. The Filter drop-down menu in the single-section reports contains the **Quick Filter** and **Advanced Filter**. In the multi-section reports, you can specify only advanced filters.

Step 1 Choose **Operations** > **Reports** and click the required report.

Step 2 In the **Filters** section, from the **Match** drop-down list, choose one of the options.

a) Choose **All** to match all specified conditions.

b) Choose **Any** to match any one specified condition.

Step 3 From the **Time Range** drop-down list, choose the required category.

Step 4 From the **Operator Commands** drop-down list, choose the required command. For example, you can filter text that begins with a specific character (use Begin With), or specific characters anywhere in the text (use Contains). Or, you can choose the Logged Time and corresponding Custom option and specify the From and To date and time from the calendar to filter data.

Step 5 From the **Time Range** drop-down list, choose the required option.

Step 6 Click **Go**.

You can save a filtered report and retrieve it from the **Filter** drop-down list for future reference.

Run and View Reports

This section describes how to run, view, and navigate reports using Reports View. When you click a report, by default, data for the last seven days is generated. Each report displays 1000 rows of data per page. You can specify time increments over which to display data in a report.

Step 1 Choose **Operations** > **Reports** > **ISE Reports**.

You can also navigate to the **Reports** link under each work center to view the set of reports specific to that work center.

Step 2 Click a report from the **report** categories available.

Step 3 Select one or more filters to run a report. Each report has different filters available, of which some are mandatory and some are optional.

Step 4 Enter an appropriate value for the filters.

Step 5 Click **Go**.

Related Topics

Export Reports, on page 4
Available Reports, on page 7

Reports Navigation

You can get detailed information from the reports output. For example, if you have generated a report for a period of five months, the graph and table will list the aggregate data for the report in a scale of months.

You can click a particular value from the table to see another report related to this particular field. For example, an authentication summary report will display the failed count for the user or user group. When you click the failed count, an authentication summary report is opened for that particular failed count.

Export Reports

You can export report data in the following file formats:

- Excel spreadsheet as a Comma Separated Values (.csv) file. After you export the data, you will receive an email detailing the location of the report.
- Microsoft Excel Comma Separated Values (CSV) file that can be saved to a local disk.
- Adobe Acrobat Document (.pdf) file that can be saved to a local disk.

You can only export the PDF file format of the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary

Note Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.

- Guest Sponsor summary
- End point Profile Changes
- Network Device Session Status

Note To view the non-English characters correctly after exporting a report, you must import the file into Microsoft Excel by enabling UTF-8 character encoding. If you choose to open the exported .csv file directly in Microsoft Excel without enabling UTF-8 character encoding, the non-English characters in the report might appear in some garbage form.

Note You can export report data to a .csv format only from the Primary PAN.

Step 1 Run a report, as described in the Running and Viewing Reports section.

Step 2 Click **Export To** in the top-right corner of the report summary page.

Step 3 Specify the data columns that you want to export.

Step 4 Choose a repository from the drop-down list.

Step 5 Click **Export** .

Step 6 Choose one of the following options:

- Repository (CSV): To export the report in CSV file format to a repository

- Local (CSV): To export the report in CSV file format to a local disk
- Local (PDF): To export the report in pdf file format to a local disk

Note
- When you select the local CSV or pdf option, only the first 500 records are exported. You can use the Repository CSV option to export all the records.
- When you export the multi-section reports using the local pdf option, only the first 100 rows are exported for each section.

Schedule and Save Cisco ISE Reports

You can customize a report and save the changes as a new report, or restore the default report settings in **My Reports** at the top right corner of the report summary page.

You can also customize and schedule Cisco ISE reports to run and re-run at specific time or time intervals. You can also send and receive email notifications for the reports generated.

When scheduling reports with **Hourly** frequency, you can have the report run over multiple days, but the timeframe cannot spread across two days.

For example, when scheduling an hourly report from May 4, 2019, to May 8, 2019, you can set the time interval as between 6:00 a.m. and 11:00 p.m. each day, but not between 6:00 p.m. of one day and 11:00 a.m. of the next. Cisco ISE displays an error message that the time range is invalid in the latter case.

Note If an external administrator (for example: Active Directory Administrator) creates a scheduled report without filling the email-id field, no email notifications will be sent.

You cannot schedule the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary
- Guest Sponsor summary
- Endpoint Profile Changes
- Network Device Session Status

Note You can save or schedule (customize) Cisco ISE reports only from the PAN.

Step 1 Run a report as described in the Running and Viewing Reports section.

Step 2 Click **My Reports** in the top right-hand corner of the report summary page.

Step 3 Enter the required details in the dialog box.

Step 4 Click **Save as New**.

When you go back to a saved report, all the filter options are checked by default. Uncheck the filters that you do not wish to use.

You can also remove a saved report from **My Reports** category.

Cisco ISE Active RADIUS Sessions

Cisco ISE provides a dynamic Change of Authorization (CoA) feature for the Live Sessions that allows you to dynamically control active RADIUS sessions. You can send reauthenticate or disconnect requests to a Network Access Device (NAD) to perform the following tasks:

- Troubleshoot issues related to authentication—You can use the Session reauthentication option to follow up with an attempt to reauthenticate again. However, you must not use this option to restrict access. To restrict access, use the shutdown option.
- Block a problematic host—You can use the Session termination with port shutdown option to block an infected host that sends a lot of traffic over the network. However, the RADIUS protocol does not currently support a method for re-enabling a port that has been shut down.
- Force endpoints to reacquire IP addresses—You can use the Session termination with port bounce option for endpoints that do not have a supplicant or client to generate a DHCP request after a VLAN change.
- Push an updated authorization policy to an endpoint—You can use the Session reauthentication option to enforce an updated policy configuration, such as a change in the authorization policy on existing sessions based on the discretion of the administrator. For example, if posture validation is enabled, when an endpoint gains access initially, it is usually quarantined. After the identity and posture of the endpoint are known, it is possible to send the Session reauthentication command to the endpoint for the endpoint to acquire the actual authorization policy based on its posture.

For CoA commands to be understood by the device, it is important that you configure the options appropriately.

For CoA to work properly, you must configure the shared secret of each device that requires a dynamic change of authorization. Cisco ISE uses the shared secret configuration to request access from the device and issue CoA commands to it.

Note In this release of Cisco ISE, the maximum number of active authenticated endpoint sessions that can be displayed is limited to 100,000.

Related Topics

Change Authorization for RADIUS Sessions, on page 7

Change Authorization for RADIUS Sessions

Some Network Access Devices on your network may not send an Accounting Stop or Accounting Off packet after a reload. As a result, you might find two sessions in the Session Directory reports, one which has expired.

To dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session, be sure to choose the most recent session.

Step 1 Choose **Operations** > **RADIUS Livelog**.

Step 2 Switch the view to **Show Live Session**.

Step 3 Click the CoA link for the RADIUS session that you want to issue CoA and choose one of the following options:

- **SAnet Session Query**—Use this to query information about sessions from SAnet supported devices.
- **Session reauthentication**—Reauthenticate session. If you select this option for a session established on an ASA device supporting COA, this will invoke a Session Policy Push CoA.
- **Session reauthentication with last**—Use the last successful authentication method for this session.
- **Session reauthentication with rerun**—Run through the configured authentication method from the beginning.

  Note **Session reauthentication with last** and **Session reauthentication with rerun** options are not currently supported in Cisco IOS software.

- **Session termination**—Just end the session. The switch reauthenticates the client in a different session.
- **Session termination with port bounce**—Terminate the session and restart the port.
- **Session termination with port shutdown**—Terminate the session and shutdown the port.

Step 4 Click **Run** to issue CoA with the selected reauthenticate or terminate option.

If your CoA fails, it could be one of the following reasons:

- Device does not support CoA.
- Changes have occurred to the identity or authorization policy.
- There is a shared secret mismatch.

Available Reports

The following table lists the preconfigured reports, grouped according to their category. Descriptions of the report functionality and logging category are also provided.

To generate syslogs for a logging category, set its **Log Severity Level** to **Info**:

- Choose **Administration > System > Logging > Logging Categories**.
- Click the logging category for which syslogs must be generated.
- From the **Log Severity Level** drop-down list, choose **Info**.

- Click **Save**.

Report Name	Description	Logging Category
Audit		
Adaptive Network Control Audit	The Adaptive Network Control Audit report is based on RADIUS accounting. It displays historical reporting of all the network sessions for each endpoint.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Passed Authentications and RADIUS Accounting.
Administrator Logins	The Administrator Logins report provides information about all the GUI-based administrator login events as well as successful CLI login events.	Choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Administrative and Operational Audit**.
Change Configuration Audit	The Change Configuration Audit report provides details about configuration changes within a specified time period. If you need to troubleshoot a feature, this report can help you determine if a recent configuration change contributed to the problem.	Choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Administrative and Operational Audit**.

Report Name	Description	Logging Category
Data Purging Audit	The Data Purging Audit report records when the logging data is purged. This report reflects two sources of data purging. At 4 a.m. daily, Cisco ISE checks whether there are any logging files that meet the criteria you have set on the **Administration > Maintenance > Data Purging** window. If yes, the files are deleted and recorded in this report. Additionally, Cisco ISE continually maintains a maximum of 80 percent used storage space (threshold) for the log files. Every hour, Cisco ISE verifies this percentage and deletes the oldest data until this threshold is reached again. This information is also recorded in this report. If there is high disk space utilization, an alert message stating `ISE Monitor node(s) is about to exceed the maximum amount allocated` is displayed at 80 percent of the threshold, that is 60 percent of total disk space. Subsequently, an alert message stating `ISE Monitor node(s) has exceeded the maximum amount allocated` is displayed at 90 percent of the threshold, that is 70 percent of the total disk space.	—
Endpoints Purge Activities	The Endpoints Purge Activities report enables a user to review the history of endpoints purge activities. This report requires that the Profiler logging category is enabled. (Note that this category is enabled by default.)	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Profiler.

Report Name	Description	Logging Category
Internal Administrator Summary	The Internal Administrator Summary report enables you to verify the entitlement of administrator users. From this report, you can also access the Administrator Logins and Change Configuration Audit reports, which enables you to view these details for each administrator.	—
Operations Audit	The Operations Audit report provides details about any operational changes, such as, running backups, registering a Cisco ISE node, or restarting an application.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Administrative and Operational audit.
pxGrid Administrator Audit	The pxGrid Administrator Audit report provides details of the pxGrid administration actions, such as client registration, client deregistration, client approval, topic creation, topic deletion, publisher-subscriber addition, and publisher-subscriber deletion on the Primary PAN. Every record has the name of the administrator who has performed the action on the node. You can filter the pxGrid Administrator Audit report based on the administrator and message criteria.	—
Secure Communications Audit	The Secure Communications Audit report provides auditing details about security-related events in Cisco ISE Admin CLI, which includes authentication failures, possible break-in attempts, SSH logins, failed passwords, SSH logouts, invalid user accounts, and so on.	—
User Change Password Audit	The User Change Password Audit report displays verification about employees' password changes.	
Device Administration		

Report Name	Description	Logging Category
TACACS Accounting	The TACACS Accounting report provides accounting details for a device session. It displays information related to the generated and logged time of the users and devices.	Choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **TACACS Accounting**.
Diagnostics		
AAA Diagnostics	The AAA Diagnostics report provides details of all the network sessions between Cisco ISE and users. If users cannot access the network, you can review this report to identify trends and identify whether the issue is isolated to a particular user or indicative of a more widespread problem. **Note** Sometimes ISE will silently drop the Accounting Stop request of an endpoint if user authentication is in progress. However, ISE starts acknowledging all the accounting requests after user authentication is completed.	Choose **Administration** > **System** > **Logging** > **Logging Categories**, and select the following logging categories: **Policy Diagnostics**, **Identity Stores Diagnostics**, **Authentication Flow Diagnostics**, and **RADIUS Diagnostics**.
AD Connector Operations	The AD Connector Operations report provides log of operations performed by the AD Connector, such as Cisco ISE Server password refresh, Kerberos tickets management, DNS queries, DC discovery, LDAP, RPC Connections management, and so on. If some AD failures are encountered, you can review the details in this report to identify the possible causes.	Choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **AD Connector**.
Endpoint Profile Changes	The Top Authorization by Endpoint (MAC address) report displays how many times each endpoint MAC address was authorized by Cisco ISE to access the network.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **Passed Authentications** and **Failed Attempts**.

Report Name	Description	Logging Category
Health Summary	The Health Summary report provides details similar to the Dashboard. However, the Dashboard only displays data for the past 24 hours. Also, you can review more historical data using this report. You can evaluate this data to see consistent patterns in data. For example, you would expect heavier CPU usage when most employees start their work days. If you see inconsistencies in these trends, you can identify potential problems. The CPU Usage table lists the percentage of CPU usage for the different Cisco ISE functions. The output of the **show cpu usage** CLI command is presented in this table and you can correlate these values with the issues in your deployment to identify possible causes.	—
ISE Counters	The ISE Counters report lists the threshold values for various attributes. The values for these different attributes are collected at different intervals and the data is presented in a tabular format; one at 5-minute interval and another after 5 minutes. You can evaluate this data to see the trend, and if you find values that are higher than the threshold, you can correlate this information with the issues in your deployment to identify possible causes. By default, Cisco ISE collects the values for these attributes. You can choose to disable this data collection from the Cisco ISE CLI using the **application configure ise** command. Choose **option 14** to enable or disable counter attribute collection.	—

Report Name	Description	Logging Category
Key Performance Metrics	The Key Performance Metrics report provides statistical information about the number of endpoints that connect to your deployment and the amount of RADIUS requests that are processed by each of the PSNs on an hourly basis. This report lists the average load on the server, average latency per request, and the average transactions per second.	—
Misconfigured NAS	The Misconfigured NAS report provides information about NADs with inaccurate accounting frequency, typically when sending accounting information frequently. If you have taken corrective actions and fix the misconfigured NADs, the report displays fixed acknowledgment in the report. **Note** **RADIUS Suppression** should be enabled to run this report.	—
Misconfigured Supplicants	The Misconfigured Supplicants report provides a list of misconfigured supplicants along with the statistics because of failed attempts that are performed by a specific supplicant. If you have taken corrective actions and fix the misconfigured supplicant, the report displays fixed acknowledgment in the report. **Note** **RADIUS Suppression** should be enabled to run this report.	—

Report Name	Description	Logging Category
Network Device Session Status	The Network Device Session Status Summary report enables you to display switch configuration without logging in to the switch directly. Cisco ISE accesses these details using an SNMP query and requires that your network devices are configured with SNMP v1 or v2c. If a user is experiencing network issues, this report can help you identify if the issue is related to switch configuration or with Cisco ISE.	—
OCSP Monitoring	The OCSP Monitoring Report specifies the status of the Online Certificate Status Protocol (OCSP) services. It identifies whether Cisco ISE can successfully contact a certificate server, and provides certificate status auditing. It also provides a summary of all the OCSP certificate-validation operations performed by Cisco ISE. It retrieves information related to the good and revoked primary and secondary certificates from the OCSP server. Cisco ISE caches the responses and utilizes them for generating subsequent OCSP Monitoring Reports. In the event the cache is cleared, it retrieves information from the OCSP server.	Choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **System Diagnostics**.
RADIUS Errors	The RADIUS Errors report enables you to check for RADIUS Requests Dropped (authentication or accounting requests that are discarded from unknown Network Access Device), EAP connection time outs, and unknown NADs. **Note** You can view the report only for the past 5 days.	Choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **Failed Attempts**.

Report Name	Description	Logging Category
System Diagnostics	The System Diagnostic report provides details about the status of the Cisco ISE nodes. If a Cisco ISE node is unable to register, you can review this report to troubleshoot the issue. This report requires that you first enable several diagnostic logging categories. Collecting these logs can negatively impact Cisco ISE performance. So, these categories are not enabled by default, and you should enable them just long enough to collect the data. Otherwise, they are automatically disabled after 30 minutes.	Choose **Administration** > **System** > **Logging** > **Logging Categories**, and select the following logging categories: **Internal Operations Diagnostics**, **Distributed Management**, and **Administrator Authentication and Authorization**.
Endpoints and Users		
Authentication Summary	The Authentication Summary report is based on the RADIUS authentications. It enables you to identify the most common authentications and the reason for authentication failures, if any. For example, if one Cisco ISE server is handling significantly more authentications than others, you might want to reassign users to different Cisco ISE servers to better balance the load. **Note** Because the Authentication Summary report or dashboard collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.	—

Report Name	Description	Logging Category
Client Provisioning	The Client Provisioning report indicates the client provisioning agents applied to particular endpoints. You can use this report to verify the policies applied to each endpoint, and in turn, use this to verify whether the endpoints have been correctly provisioned. **Note** The MAC address of an endpoint is not displayed in the **Endpoint ID** column if the endpoint does not connect with ISE (no session is established), or if a Network Address Translation (NAT) address is used for the session.	Choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **Posture and Client Provisioning Audit** and **Posture and Client Provisioning Diagnostics**.
Current Active Sessions	The Current Active Sessions report enables you to export a report with details about who is on the network within a specified time period. If a user isn't getting network access, you can see whether the session is authenticated or terminated, or if there is another problem with the session.	—
External Mobile Device Management	The External Mobile Device Management report provides details about integration between Cisco ISE and the external Mobile Device Management (MDM) server. You can use this report to see which endpoints have been provisioned by the MDM server without logging into the MDM server directly. It also displays information such as registration and MDM-compliance status.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select MDM.

Report Name	Description	Logging Category
Passive ID	The Passive ID report enables you to monitor the state of WMI connection to the domain controller and gather statistics related to it (such as amount of notifications received, amount of user login/logouts per second etc.) **Note** Sessions authenticated by this method do not have authentication details in the report.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Identity Mapping.
Manual Certificate Provisioning	The Manual Certificate Provisioning report lists all the certificates that are provisioned manually via the certificate provisioning portal.	—
Posture Assessment by Condition	The Posture Assessment by Condition report enables you to view records based on the posture policy condition configured in ISE to validate that the most up-to-date security settings or applications are available on client machines.	—
Posture Assessment by Endpoint	The Posture Assessment by Endpoint report provides detailed information, such as the time, status, and PRA Action, of an endpoint. You can click **Details** to view further information of an endpoint.	—
Profiled Endpoints Summary	The Profiled Endpoints Summary report provides profiling details about endpoints that are accessing the network. **Note** For endpoints that do not register a session time, such as a Cisco IP-Phone, the term Not Applicable is shown in the Endpoint session time field.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Profiler.

Report Name	Description	Logging Category
RADIUS Accounting	The RADIUS Accounting report identifies how long users have been on the network. If users are losing network access, you can use this report to identify whether Cisco ISE is the cause of the network connectivity issues. **Note** Radius accounting interim updates are included in the RADIUS Accounting report if the interim updates contain information about the changes to the IPv4 or IPv6 addresses for the given sessions.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select RADIUS Accounting. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select RADIUS Accounting.
RADIUS Authentications	The RADIUS Authentications report enables you to review the history of authentication failures and successes. If users cannot access the network, you can review the details in this report to identify possible causes.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select these logging categories: Passed Authentications and Failed Attempts.
Registered Endpoints	The Registered Endpoints report displays all personal devices registered by employees.	—
Rejected Endpoints	The Rejected Endpoints report lists all rejected or released personal devices that are registered by employees. The data for this report will be available only when you install the Plus license.	—
Supplicant Provisioning	The Supplicant Provisioning report provides details about the supplicants provisioned to employee's personal devices.	Posture and Client Provisioning Audit
Top Authorizations by Endpoint	The Top Authorization by Endpoint (MAC address) report displays how many times each endpoint MAC address was authorized by Cisco ISE to access the network.	Passed Authentications, Failed Attempts

Report Name	Description	Logging Category
Top Authorizations by User	The Top Authorization by User report displays how many times each user was authorized by Cisco ISE to access the network.	Passed Authentications, Failed Attempts
Guest		
AUP Acceptance Status	The AUP Acceptance Status report provides details of AUP acceptances from all the Guest portals.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Guest.
Guest Accounting	The Guest Accounting report is a subset of the RADIUS Accounting report. All users assigned to the Activated Guest or Guest identity groups appear in this report.	—

Report Name	Description	Logging Category
Master Guest Report	The Master Guest Report combines data from various Guest Access reports and enables you to export data from different reporting sources. The Master Guest report also provides details about the websites that guest users are visiting. You can use this report for security auditing purposes to demonstrate when guest users accessed the network and what they did on it. You must also enable HTTP inspection on the network access device (NAD) used for guest traffic. This information is sent back to Cisco ISE by the NAD. To check when the clients reach the maximum simultaneous sessions limit, from the Admin portal, choose **Administration > System > Logging > Logging Categories** and do the following: **1.** Increase the log level of "Authentication Flow Diagnostics" logging category from WARN to INFO. **2.** Change LogCollector Target from Available to Selected under the "Logging Category" of AAA Diagnostics.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Passed Authentications.
My Devices Login and Audit	The My Devices Login and Audit report provides details about the login activities and the operations performed by the users on the devices in My Devices Portal.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select My Devices.

Report Name	Description	Logging Category
Sponsor Login and Audit	The Sponsor Login and Audit report provides details of guest users' login, add, delete, enable, suspend and update operations and the login activities of the sponsors at the sponsors portal. If guest users are added in bulk, they are visible under the column 'Guest Users.' This column is hidden by default. On export, these bulk users are also present in the exported file.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Guest.
SXP		
SXP Binding	The SXP Binding report provides information about the IP-SGT bindings that are exchanged over SXP connection.	—
SXP Connection	You can use this report to monitor the status of an SXP connection and gather information related to it, such as peer IP, SXP node IP, VPN name, SXP mode, and so on.	—
Trustsec		
RBACL Drop Summary	The RBACL Drop Summary report is specific to the TrustSec feature, which is available only with an Advanced Cisco ISE license. This report also requires that you configure the network devices to send NetFlow events for dropped events to Cisco ISE. If a user violates a particular policy or access, packets are dropped and indicated in this report. **Note** Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.	—

Report Name	Description	Logging Category
Top N RBACL Drops By User	The Top N RBACL Drops By User report is specific to the TrustSec feature, which is available only with an Advanced Cisco ISE license. This report also requires that you configure the network devices to send NetFlow events for dropped events to Cisco ISE. This report displays policy violations (based on packet drops) by specific users. **Note** Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.	—
TrustSec ACI	This report lists the SGTs and SXP mappings that are synchronized with the IEPGs, EEPGs, endpoints, and subnet configuration of APIC. These details are displayed only if the TrustSec APIC integration feature is enabled.	—

Report Name	Description	Logging Category
TrustSec Deployment Verification		—

Report Name	Description	Logging Category
	You can use this report to verify whether the latest TrustSec policies are deployed on all network devices or if there are any discrepancies between the policies configured in Cisco ISE and the network devices. Click the **Details** icon to view the results of the verification process. You can view the following details: • When the verification process started and completed • Whether the latest TrustSec policies are successfully deployed on the network devices. You can also view the names and IP addresses of the network devices on which the latest TrustSec policies are deployed. • Whether if there are any discrepancies between the policies configured in Cisco ISE and the network devices. It displays the device name, IP address, and the corresponding error message for each policy difference. You can view the TrustSec Deployment Verification alarms in the **Alarms** dashlet (under **Work Centers > TrustSec > Dashboard** and **Home > Summary**). **Note** • The time taken for reporting depends on the number of network devices and TrustSec groups in your deployment. • The error message length in the TrustSec Deployment Verification report is currently limited	

Report Name	Description	Logging Category
	to 480 characters. Error messages with more than 480 characters will be truncated and only the first 480 characters will be displayed in the report.	
Trustsec Policy Download	This report lists the requests sent by the network devices for policy (SGT/SGACL) download and the details sent by ISE. If the Workflow mode is enabled, the requests can be filtered for production or staging matrix.	To view this report, you must do the following: **1.** Choose **Administration** > **System** > **Logging** > **Logging Categories**. **2.** Choose **AAA Diagnostics** > **RADIUS Diagnostics**. **3.** Set the Log Severity Level to DEBUG for RADIUS Diagnostics.
Threat Centric NAC Service		
Adapter Status	The Adapter Status report displays the status of the threat and vulnerability adapters.	—
COA Events	When a vulnerability event is received for an endpoint, Cisco ISE triggers CoA for that endpoint. The CoA Events report displays the status of these CoA events. It also displays the old and new authorization rules and the profile details for these endpoints.	—
Threat Events	The Threat Events report provides a list of all the threat events that Cisco ISE receives from the various adapters that you have configured.	—

Report Name	Description	Logging Category
Vulnerability Assessment	The Vulnerability Assessment report provides information about the assessments that are happening for your endpoints. You can view this report to check if the assessment is happening based on the configured policy.	—